二面体群へのコサイクルの個数について (有限群のコホモロジー論の研究)

AUTHOR(S):

淺井, 恒信; 竹ヶ原, 裕元; 庭崎, 隆

CITATION:

淺井, 恒信 ...[et al]. 二面体群へのコサイクルの個数について (有限群のコホモロジー論の研究). 数理解析研究所講究録 2002, 1251: 70-82

ISSUE DATE:

2002-02

URL:

http://hdl.handle.net/2433/41801

数理解析研究所講究録 1251 巻 2002 年 70-82

二面体群へのコサイクルの個数について

近畿大学・理工学部　浅井 恒信 (Tsunenobu Asai),
Department of Mathematics, Kinki Univ.
室蘭工業大学　竹ヶ原 裕元 (Yugen Takegahara),
Muroran Institute of Technology
愛媛大学・理学部　庭崎 隆 (Takashi Niwasaki),
Department of Mathematics, Ehime Univ.

1　はじめに

A, G を有限群とし, A は G に作用している, 即ち準同型 $\varphi\colon A \to \mathrm{Aut}(G)$ が与えられているものとする。$a \in A$ と $g \in G$ に対する $\varphi(a)(g) \in G$ を ${}^a g$ と書く。また, 代数的な同型のみならず, 集合 X と Y の間に全単射があるときにも $X \simeq Y$ という記号を使う。X の濃度を $|X|$ で表す。

写像 $\zeta\colon A \to G$ がコサイクル (または斜準同型, 微分) とは,

$$\zeta(ab) = \zeta(a) \cdot {}^a\zeta(b) \quad (\forall a, b \in A)$$

が成り立つときにいう。コサイクルの全体を $Z^1(A, G)$ で表す。φ が自明な作用のときは, $Z^1(A, G) = \mathrm{Hom}(A, G)$ である。G が A-加群のとき $Z^1(A, G)$ は (bar resolution に関する) 1 次のコサイクル群であるが, 一般の非可換な G に対する $Z^1(A, G)$ には群構造が知られていない。このことが以下の議論を難しくしている最大の要因といえる。

さて, 有限群上の方程式の解の個数に関する Frobenius の古典的な定理 ([4], [6], [7], [8], [9], [11])

$$\left|\{g \in G \mid g^n = 1\}\right| \equiv 0 \pmod{\gcd(n, |G|)}$$

を拡張した $|\mathrm{Hom}(A, G)|$ についての吉田 [10] による結果に関連して, 次の予想がある:

予想 ([3]). $\left|Z^1(A, G)\right| \equiv 0 \pmod{\gcd(|A/A'|, |G|)}$ が成り立つ。ここで, A' は A の交換子群を表す。

この予想は現在 A がアーベル群の場合について調べられているところで, A が素数 p に対する巡回 p-群 C と基本可換 p-群 E の直積 $C \times E$ の場合を含め, 幾つかの場合に正しいことが証明されている ([9], [3], [1], [2], [13])。

最近, これまで未解決であった場合, 即ち A が巡回群 2 個の直積 $C_1 \times C_2$ で, G が位数 $2n$ (n は 2 巾) の二面体群 D_{2n}, 準二面体群 SD_{2n}, 及び一般四元数群 Q_{2n} の場合に予想が正しいことが証明できた。本講演の目的はこのことの報告である。

アプローチとしては次の方法をとった。G の位数 n の特性巡回部分群 $\langle x \rangle$ に注目し,

(1) 巡回群 C に対する $\left|Z^1(C, \langle x \rangle)\right|$ を初等整数論的に把え, その性質を調べる。
(2) $\left|Z^1(A, \langle x \rangle)\right| \not\equiv 0 \pmod{\gcd(|A|, 2n)}$ となる場合を特徴づける。
(3) $Z^1(A, G)$ を G の剰余類によって分割し, 作用を取り換えることにより $Z^1(A, \langle x \rangle)$ の議論に帰着させる。

本稿は $G = D_{2n}$ の場合を解説したが, SD_{2n} や Q_{2n} の場合も全く平行した議論で同様に計算できる。これらの群に限らず, 一般にこの種の, 巡回群に帰着させるような局所的な議論をするときには, 上記 (1) で調べた写像 T の性質は有用だと思われる。

また, 予想を A や G の位数に関する帰納法で証明しようと試みるとき, 上記 (2) のような場合 (ある状況下で予想の記述より多くは p で割れない場合) は次のステップにとって障害となる可能性があり, このケースを正確に記述することは後々重要な意味をもってくる。このことに関連して, 次の結果がある。

定理 1.1 ([2], [13]). p を素数とし, 巡回 p-群 C が p-群 G に作用しているとする。このとき, もし

$$\left|Z^1(C,G)\right| \not\equiv 0 \pmod{\gcd(p|C|,|G|)}$$

となるならば, G は巡回群, D_{2n}, SD_{2n}, Q_{2n} の何れかである。

上記定理の主張の $p=2$ の場合は村井正文氏によって得られた。本稿は $|A|$ に関する帰納法がのりにくいであろうと思われる, これら典型的な群についての計算例である。

2 半直積とコサイクル

群 A が群 G に準同型 $\varphi\colon A \to \mathrm{Aut}(G)$ で作用しているものとする。作用 φ を強調するとき, G のことを G_φ と書く。G と A の半直積を $G \rtimes A$ で表す。群の準同型 $f\colon B \to A$ が与えられたとき, B は G に合成写像 φf で作用する。次は (少くとも G が A-加群のときは) よく知られていると思われる ([5, IV 章], [12, 第 2 章 §8] 等)。

定理 2.1. 群 B に対して,

$$\mathrm{Hom}(B, G_\varphi \rtimes A) = \left\{\zeta \rtimes f \;\middle|\; f \in \mathrm{Hom}(B,A),\ \zeta \in Z^1(B, G_{\varphi f})\right\}$$

である。但し, ここで $(\zeta \rtimes f)(b) := (\zeta(b), f(b))$ $(b \in B)$ である。

系 2.2. $\pi\colon G \rtimes A \to A$ を自然な全射とする。このとき, 次のような全単射がある。

$$Z^1(A,G) \overset{\Phi}{\simeq} \left\{\theta \in \mathrm{Hom}(A, G \rtimes A) \;\middle|\; \pi\theta = \mathrm{id}_A\right\} \overset{\Psi}{\simeq} \left\{B \leq G \rtimes A \;\middle|\; GB = G \rtimes A,\ G \cap B = 1\right\}$$

対応は $\zeta \in Z^1(A,G)$ に対して $\Phi(\zeta) := \zeta \rtimes \mathrm{id}_A$, 及び $\theta \in \mathrm{Hom}(A, G \rtimes A)$ に対して $\Psi(\theta) := \theta(A)$ である。

この系の一つめの対応 Φ から, $Z^1(A,G) \subset \mathrm{Hom}(A, G \rtimes A)$ とみなすことができる。このことから, A の生成集合 S とその基本関係 R が与えられたとき, 準同型の場合と同様に, コサイクルを以下のように S の各元の行き先と関係 R の言葉で表すことができる。

$A = \langle S \mid R\rangle$ とし, S 上の自由群を F とおく。A の G 上の作用は, F の G 上の作用を自然に引き起こす。写像 $\zeta_S\colon S \to G$ が与えられたとき, $S \cup S^{-1} (\subset F)$ の元の有限列全体から G への写像 ζ_F を

$$\zeta_F(s) := \zeta_S(s), \quad \zeta_F(s^{-1}) := {}^{s^{-1}}(\zeta_S(s)^{-1}) \qquad (s \in S),$$
$$\zeta_F(s_1, s_2, \ldots, s_n) := \zeta_F(s_1) \cdot {}^{s_1}\zeta_F(s_2, \ldots, s_n) \qquad (s_1, \ldots, s_n \in S \cup S^{-1})$$

により帰納的に定義する。このとき, 自然に $\zeta_F \in Z^1(F,G)$ とみなせ, 更に次が成り立つ。

定理 2.3. $A = \langle S \mid R\rangle$ ならば, 自然な全単射 $Z^1(A,G) \simeq \left\{\zeta_S\colon S \to G \;\middle|\; \zeta_F(R) = 1\right\}$ がある。

例 2.4. (1) $A = \langle c \mid c^m = 1\rangle$ とする。コサイクル $\zeta\colon A \to G$ を与えることは準同型 $\zeta \rtimes \mathrm{id}_A\colon A \to G \rtimes A$ を与えること, 即ち $(g,c)^m = 1$ となる $(g,c) \in G \rtimes A$ を与えることと同値である。自然数 i に対し,

$$R(g,c,i) := g \cdot {}^c g \cdot {}^{c^2} g \cdot \cdots \cdot {}^{c^{i-1}} g$$

とおけば, $(g,c)^i = (R(g,c,i), c^i)$ であるから,

$$Z^1(C,G) \simeq \left\{g \in G \;\middle|\; R(g,c,m) = 1\right\}$$

(2) 同様に, $A = \langle c_1, c_2 \mid c_1^{m_1} = c_2^{m_2} = 1,\ c_1c_2 = c_2c_1\rangle$ $(= \langle c_1\rangle \times \langle c_2\rangle)$ のとき,

$$Z^1(A,G) \simeq \left\{(g_1,g_2) \in G \times G \;\middle|\; R(g_1,c_1,m_1) = R(g_2,c_2,m_2) = 1,\ g_1 \cdot {}^{c_1} g_2 = g_2 \cdot {}^{c_2} g_1\right\}$$

次に系 2.2 の二つめの対応 Ψ に注目する。$\zeta \in Z^1(A,G)$ を与えることと, $G \rtimes A$ における G の補群 ($GB = G \rtimes A$, $G \cap B = 1$ となる $B \leq G \rtimes A$ のこと) を与えることとは同値であった。今, $\zeta \in Z^1(A,G)$ を一つ固定する。系 2.2 に現われた

$$A_\zeta := (\zeta \rtimes \mathrm{id}_A)(A) = \{(\zeta(a), a) \in G \rtimes A \mid a \in A\}$$

は $G \rtimes A$ における G の補群であり, $G \rtimes A = GA_\zeta \simeq G \rtimes A_\zeta$ である (但し, 右辺における A_ζ の作用は $G \rtimes A$ 内における共役である)。従って, $G \rtimes A$ において G の補群を与えることと, $G \rtimes A_\zeta$ において G の補群を与えることとは同値である。故に $Z^1(A,G) \simeq Z^1(A_\zeta, G)$ となる。

以上のことを $A \simeq A_\zeta \to \mathrm{Aut}(G)$ という A の作用としてまとめると, 次の「作用の取り換え」に関する定理を得る。

定理 2.5. $\zeta \in Z^1(A, G_\varphi)$ とすると, 新しい作用

$$\zeta * \varphi \colon A \to \mathrm{Aut}(G), \qquad {}^{(\zeta*\varphi)(a)}g := \zeta(a) \cdot {}^{\varphi(a)}g \cdot \zeta(a)^{-1} \quad (a \in A,\ g \in G)$$

を定義でき, 次は全単射になる:

$$\zeta_r \colon Z^1(A, G_{\zeta*\varphi}) \longrightarrow Z^1(A, G_\varphi), \qquad \eta \mapsto \eta \cdot \zeta \quad (\text{但し, } (\eta \cdot \zeta)(a) := \eta(a)\zeta(a))$$

3 $Z^1(C, \langle x \rangle)$

以下, 本稿を通して次の記号を用いる。自然数 n に対して, $\mathbf{Z}_n = \mathbf{Z}/(n)$ とおき, その単数群を $U(\mathbf{Z}_n)$ で表す。$m \in \mathbf{Z}$ に対し, m と n の正の最大公約数を m_n で表す:

$$m_n := \gcd(m, n) \in \mathbf{Z}$$

$0_n = n$ である。また, n が p 巾のとき, m_n は m の (n を上限とする) p-part である。

更に $m \in \mathbf{Z}_n$ のときも, m を整数値とみて n との最大公約数をとり, それを m_n で表す。m_n は m の代表元の取り方によらず一意に定まる n の約数である。m_n を再び法 n で考えれば, $\mathbf{Z}_n$ のイデアルとして $(m) = (m_n)$ であり, m の $\mathbf{Z}_n$ における零化イデアルを $\mathrm{Ann}_{\mathbf{Z}_n}(m)$ で表せば, $|\mathrm{Ann}_{\mathbf{Z}_n}(m)| = m_n$ である。

3.1 一般の場合

本節では有限巡回群 $C = \langle c \rangle$ が位数 n の巡回群 $\langle x \rangle$ に,

$$\varphi \colon C \to U(\mathbf{Z}_n) \simeq \mathrm{Aut}(\langle x \rangle), \qquad c \mapsto a$$

で作用している場合を考える。即ち,

$${}^c x = x^a, \qquad a \in U(\mathbf{Z}_n)$$

であり, a の $U(\mathbf{Z}_n)$ における位数 $|a|$ は $|C|$ の約数となっている状況を考える。例 2.4 の記号の下,

$$Z^1(C, \langle x \rangle) \simeq \{x^j \mid R(x^j, c, |C|) = 1\}, \qquad \text{但し} \quad R(x^j, c, |C|) = x^{j \sum_{i=0}^{|C|-1} a^i}$$

である。そこで, 一般に $k \geq 0$ に対して, 写像 $\mathrm{tr}_k \colon \mathbf{Z}_n \to \mathbf{Z}_n$ を

$$\mathrm{tr}_k(a) = \sum_{i=0}^{k-1} a^i = 1 + a + \cdots + a^{k-1} \qquad (a \in \mathbf{Z}_n)$$

で定め, その性質を調べる。$\mathrm{tr}_0(a) = 0$ であること, 及び tr_k は一般には和・積を保たないことに注意する。

補題 3.1. $k,l \geq 0$ と $a \in \mathbb{Z}_n$ に対して, 次が成り立つ。

(1) $\mathrm{tr}_{kl}(a) = \mathrm{tr}_k(a)\,\mathrm{tr}_l(a^k)$
(2) $a^k = 1$ のとき, $\mathrm{tr}_{kl}(a) = \mathrm{tr}_k(a)l$

今, $a \in U(\mathbb{Z}_n)$ に対して,

$$T(a) := \mathrm{tr}_{|a|}(a)$$

とおく。本節冒頭の設定 $|C| = |a| \cdot \frac{|C|}{|a|}$ にこの補題を適用すれば,

$$\mathrm{tr}_{|C|}(a) = T(a)\frac{|C|}{|a|}$$

であるから, $T(a)$ は $\mathrm{tr}_{|C|}(a)$ の本質的な部分を表していると考えられる。

$$Z^1(C,\langle x\rangle) \simeq \left\{x^j \mid x^{j\,\mathrm{tr}_{|C|}(a)} = 1\right\} \simeq \mathrm{Ann}_{\mathbf{Z}_n}(\mathrm{tr}_{|C|}(a)) = \mathrm{Ann}_{\mathbf{Z}_n}(\frac{|C|}{|a|}T(a))$$

であるから, 次を得る。

定理 3.2. 有限巡回群 C が位数 n の巡回群 $\langle x\rangle$ に ${}^c x = x^a$ $(a \in U(\mathbb{Z}_n))$ で作用しているとすると,

$$Z^1(C,\langle x\rangle) \simeq \mathrm{Ann}_{\mathbf{Z}_n}(\frac{|C|}{|a|}T(a)), \qquad \left|Z^1(C,\langle x\rangle)\right| = \left(\frac{|C|}{|a|}T(a)\right)_n$$

特に, $T(a)_n$ は作用 φ が忠実 (即ち $|C| = |a|$) なときのコサイクルの個数を表している。さて, 次の定理から本稿の主題が始まる。

定理 3.3. $a \in U(\mathbb{Z}_n)$ のとき, $\mathbb{Z}_n$ のイデアルとして $(T(a)) \subset (|a|)$ である。換言すると, 整数値として

$$|a|_n \mid T(a)_n$$

この一見奇妙な主張は, 自然な環準同型 $\mathbb{Z}_n \to \mathbb{Z}_{|a|_n}$ に帰納法を適用して証明することができる。この二つの定理を見比べると, 予想の最も易しい場合が確かめられる。

定理 3.4. $\left|Z^1(C,\langle x\rangle)\right| \equiv 0 \pmod{|C|_n}$。

以上, コサイクルの個数を評価したわけだが, ここで重要なことが 2 点ある。一つは, 今の設定で作用の核 $\mathrm{Ker}\,\varphi$ についての問題である。$|\mathrm{Ker}\,\varphi| = \frac{|C|}{|a|}$ であるから, 定理 3.2 より,

$$\left|Z^1(C,\langle x\rangle)\right| = \left(|\mathrm{Ker}\,\varphi| \cdot \left|Z^1(\langle a\rangle,\langle x\rangle)\right|\right)_n$$

を得る。即ち大雑把に言えば, $\left|Z^1(C,\langle x\rangle)\right|$ は作用が忠実な場合の値 $\left|Z^1(\langle a\rangle,\langle x\rangle)\right|$ の $|\mathrm{Ker}\,\varphi|$ 倍 (を n で調整したもの) であることがわかる。このことは一般の有限群については確かめられていない。

もう一つは, 予想の記述が合同式ではなく等号の場合, 即ち, いつ

$$\left|Z^1(C,\langle x\rangle)\right| = |C|_n$$

となるか, という問題である。この種の問題は §1 の最後で述べたことと関わっていて, この特別な場合について理解を深めることが次のステップで意味をもってくることがある。実際, 本稿の議論では $Z^1(C,\langle x\rangle)$ についてはさほど目立たないものの, $Z^1(C_1 \times C_2,\langle x\rangle)$ に関するこの種のこと (定理 4.3) は $\langle x\rangle$ を D_{2n} に取り換えるとき本質的な役割を果たす (命題 6.3, 定理 6.4)。そこで次節では n が 2 巾の場合に, $T(a)_n$ のもつ性質を比 $T(a)_n/|a|_n$ との関連の上で調べていく。

3.2 2 巾の場合

以下, n (>1) は 2 巾とする。$U(\mathbb{Z}_n)=\langle 5\rangle\times\langle -1\rangle$ である ($n=4$ のときは $5=1$, $n=2$ のときは $5=-1=1$ とみる)。次の表は $a\in U(\mathbb{Z}_n)$ に対する $T(a)$ の一覧である。各々の表において, $T(a)$ はなかなか面白い値をとっていることがわかる。

まず, $T(a)$ は法 n で $|a|$ の倍数である, というのが定理 3.3 である。また, 奇妙な対称性にも気づく。例えば, $a=\pm 1,3$ の三行を除くと, $T(a)$ は $a=\frac{n}{2}+1$ の行を軸に上下で対称である: $T(2-a)=T(a)$ (一般には $|2-a|\neq|a|$ である)。更に, $a\notin\langle 5\rangle$ (即ち $a\equiv 3 \mod (4)$) に対する $T(a)$ はほぼ一定である, 等々。

$[n=8]$

a	$\lvert a\rvert$	$T(a)$	$T(a)_n/\lvert a\rvert$
$1=5^0$	1	1	1
3	2	4	2
$5=5^1$	2	6	1
7	2	0	4

$[n=16]$

a	$\lvert a\rvert$	$T(a)$	$T(a)_n/\lvert a\rvert$
$1=5^0$	1	1	1
3	4	8	2
$5=5^1$	4	12	1
7	2	8	4
$9=5^2$	2	10	1
11	4	8	2
$13=5^3$	4	12	1
15	2	0	8

$[n=32]$

a	$\lvert a\rvert$	$T(a)$	$T(a)_n/\lvert a\rvert$
$1=5^0$	1	1	1
3	8	16	2
$5=5^1$	8	24	1
7	4	16	4
$9=5^6$	4	20	1
11	8	16	2
$13=5^7$	8	24	1
15	2	16	8
$17=5^4$	2	18	1
19	8	16	2
$21=5^5$	8	24	1
23	4	16	4
$25=5^2$	4	20	1
27	8	16	2
$29=5^3$	8	24	1
31	2	0	16

これらは次のことから説明がつく。例えば, $n=16$ の表をよく見ると, $a=\pm 1$ の行を除いたものは, $n=32$ の表の上下 2 箇所に, $|a|$ と $T(a)$ の値をそれぞれ 2 倍した形で現れている。つまり, 逆に言って,

補題 3.5. $\mathbb{Z}_n, \mathbb{Z}_{n/2}$ における T をそれぞれ $T_n, T_{n/2}$ で表す。また, $\pi\colon \mathbb{Z}_n\to\mathbb{Z}_{n/2}$ を自然な環準同型とする。

(1) $a\in U(\mathbb{Z}_n)$ の位数が 4 以上 (即ち $\pi(a)\neq\pm 1$) ならば,

$$|a|=2|\pi(a)|,\quad T_n(a)=2T_{n/2}(\pi(a))$$

ここで後者の右辺の意味は, $T_{n/2}(\pi(a))$ を法 $\frac{n}{2}$ を除いて決まる整数値とみたときの 2 倍 (それは法 n を除いて決まる) の $\mathbb{Z}_n$ での値のことである。

(2) 位数 2 以下の a については,

$$T_n(1)=1,\quad T_n(-1+\frac{n}{2})=\frac{n}{2},\quad T_n(1+\frac{n}{2})=2+\frac{n}{2},\quad T_n(-1)=0$$

である (但し, $a=-1$ については $n\geq 4$ のとき, $a=\pm 1+\frac{n}{2}$ については $n\geq 8$ のときの値)。

証明は補題 3.1 からすぐ出る。この補題により, $|a|$ や $T(a)$ の値は帰納的に求まる (n が 2 倍になれば, これらも概ね 2 倍になる) ことがわかり, 先に述べた対称性や次の命題も示すことができる。

命題 3.6. $a \in U(\mathbb{Z}_n)$ に対する $T(a)_n$, $T(a)_n/|a|$ は次の表のようになる:

a	$T(a)_n$	$T(a)_n/\|a\|$
$a \in \langle 5 \rangle$	$\|a\|$	1
$a \notin \langle 5 \rangle \cup \{-1\}$	$\frac{n}{2}$	$\frac{n}{2\|a\|}$
-1 (但し, $n \geq 4$)	n	$\frac{n}{2}$

命題 3.7. $a \in U(\mathbb{Z}_n)$ に対し, 次が成り立つ。

(1) $\dfrac{T(a)_n}{|a|} = \dfrac{(1+a)_n}{2}$

(2) $(1-a)_n \cdot T(a)_n = \begin{cases} 2n & (n \geq 4 \text{ かつ } a_1 = -1) \\ n & (\text{その他}) \end{cases}$, $\mathrm{Ann}_{\mathbb{Z}_n}(T(a)) = \begin{cases} \mathbb{Z}_n & (n \geq 4 \text{ かつ } a_1 = -1) \\ (1-a) & (\text{その他}) \end{cases}$

証明. $a \neq \pm 1$ について示せば十分であろう。補題 3.1 と 命題 3.6 を使う。

(1) $a^2 \in \langle 5 \rangle$ より $T(a^2)_n = |a^2|$ だから, $n > T(a)_n = ((1+a) \cdot T(a^2))_n = (1+a)_n \cdot |a^2| = (1+a)_n \cdot |a|/2$。
(2) $a \neq \pm 1$ より, $n \geq (1-a)_n \cdot (1+a)_n = (1-a^2)_n$ である。従って,

$$(1-a)_n \cdot T(a)_n = (1-a)_n \cdot (1+a)_n \cdot T(a^2)_n = (1-a^2)_n \cdot T(a^2)_n = \cdots = (1-1)_n \cdot T(1)_n = n \quad \square$$

注. n が奇素数 p に対する p 巾のときも同様に計算でき, 次のようになる: $a \in U(\mathbb{Z}_n)$ に対して,

$$T(a) = \begin{cases} |a| \mod n & (a \text{ が } p\text{-元のとき}) \\ 0 & (\text{そうでないとき}) \end{cases}$$

4 $Z^1(C_1 \times C_2, \langle x \rangle)$

p を素数とし, n (>1) は p 巾とする。$C_1 = \langle c_1 \rangle$, $C_2 = \langle c_2 \rangle$ を有限巡回群とし, $A = C_1 \times C_2$ が位数 n の巡回群 $\langle x \rangle$ に

$$\varphi\colon A \to U(\mathbb{Z}_n), \qquad \varphi(c_1) = a_1, \quad \varphi(c_2) = a_2$$

で作用しているときの $Z^1(A, \langle x \rangle)$ を計算する。コサイクル $A \to \langle x \rangle$ で

$$c_1 \mapsto g_1 = x^{i_1}, \qquad c_2 \mapsto g_2 = x^{i_2}$$

となるものが存在するための $i_1, i_2 \in \mathbb{Z}_n$ に関する必要十分条件は, 例 2.4 と定理 3.2 より,

$$i_1 \in \mathrm{Ann}_{\mathbb{Z}_n}(\frac{|C_1|}{|a_1|}T(a_1)), \quad i_2 \in \mathrm{Ann}_{\mathbb{Z}_n}(\frac{|C_2|}{|a_2|}T(a_2)), \quad (1-a_2)i_1 = (1-a_1)i_2$$

である。従って,

$$Z^1(A, \langle x \rangle) \simeq \left\{ (i_1, i_2) \in \mathrm{Ann}_{\mathbb{Z}_n}(\frac{|C_1|}{|a_1|}T(a_1)) \times \mathrm{Ann}_{\mathbb{Z}_n}(\frac{|C_2|}{|a_2|}T(a_2)) \;\middle|\; (1-a_2)i_1 = (1-a_1)i_2 \right\}$$

であり, 次は pullback である (ここで $(1-a)_l$ は $(1-a)$ 倍で定義される写像):

$$\begin{array}{ccc} Z^1(A, \langle x \rangle) & \xrightarrow{\pi_1} & \mathrm{Ann}_{\mathbb{Z}_n}(\frac{|C_1|}{|a_1|}T(a_1)) \\ \downarrow{\scriptstyle \pi_2} & & \downarrow{\scriptstyle (1-a_2)_l} \\ \mathrm{Ann}_{\mathbb{Z}_n}(\frac{|C_2|}{|a_2|}T(a_2)) & \xrightarrow[(1-a_1)_l]{} & \mathbb{Z}_n \end{array}$$

今, n は p 巾であるから, $\mathbb{Z}_n$ のイデアルは包含関係について全順序集合をなしている。そこで, $\mathrm{Im}(1-a_2)_l \subseteq \mathrm{Im}(1-a_1)_l$, 即ち

$$(1-a_2)\,\mathrm{Ann}_{\mathbf{Z}_n}(\frac{|C_1|}{|a_1|}T(a_1)) \subset (1-a_1)\,\mathrm{Ann}_{\mathbf{Z}_n}(\frac{|C_2|}{|a_2|}T(a_2)) \tag{4.1}$$

と仮定してよい。よって, 上図の右下の $\mathbf{Z}_n$ を$\mathrm{Im}(1-a_1)_l$ でおきかえてよい。このとき $(1-a_1)_l$ は全射である。pullback の性質から, π_1 も全射で, かつ $\mathrm{Ker}\,\pi_1 \simeq \mathrm{Ker}(1-a_1)_l$ なので,

$$|Z^1(A,\langle x\rangle)| = |\mathrm{Im}(\pi_1)|\cdot|\mathrm{Ker}(\pi_1)| = \left|\mathrm{Ann}_{\mathbf{Z}_n}(\frac{|C_1|}{|a_1|}T(a_1))\right|\cdot\left|\mathrm{Ann}_{\mathbf{Z}_n}(\frac{|C_2|}{|a_2|}T(a_2))\cap\mathrm{Ann}_{\mathbf{Z}_n}(1-a_1)\right|$$

である。この最後の因子の値により場合分けする。

(i) $\mathrm{Ann}_{\mathbf{Z}_n}(\frac{|C_2|}{|a_2|}T(a_2)) \subset \mathrm{Ann}_{\mathbf{Z}_n}(1-a_1)$ の場合。

このとき, 上の pullback の図における $(1-a_1)_l$ は 0-射, 従って $(1-a_2)_l$ も 0-射であるから, この図は直積を表している: $Z^1(A,G) \simeq Z^1(C_1,G)\times Z^1(C_2,G)$。定理 3.3 より $|a_i|_n \mid T(a_i)_n$ だから

$$|Z^1(A,\langle x\rangle)| = (\frac{|C_1|}{|a_1|}T(a_1))_n\cdot(\frac{|C_2|}{|a_2|}T(a_2))_n \equiv 0 \pmod{|C_1|_n\cdot|C_2|_n}$$

(ii) $\mathrm{Ann}_{\mathbf{Z}_n}(\frac{|C_2|}{|a_2|}T(a_2)) \supset \mathrm{Ann}_{\mathbf{Z}_n}(1-a_1)$ の場合。

$\mathbb{Z}_n$ において $T(a_1)\cdot(1-a_1) = 1-a_1{}^{|a_1|} = 0$ だから,

$$|Z^1(A,\langle x\rangle)| = (\frac{|C_1|}{|a_1|}T(a_1))_n\cdot(1-a_1)_n \equiv 0 \pmod{n}$$

従って, 何れにしても予想が成り立つ ($|C_1|_n\cdot|C_2|_n \equiv 0 \pmod{|A|_n}$ に注意)。

定理 4.1. $n\ (>1)$ が p 巾のとき, $|Z^1(A,\langle x\rangle)| \equiv 0 \pmod{|A|_n}$。

これで $Z^1(A,\langle x\rangle)$ についての予想は確かめ終えたわけだが, 更にここで, $p=2$ の場合に, いつ

$$|Z^1(A,\langle x\rangle)| \equiv 0 \pmod{|A|_{2n}} \tag{4.2}$$

となるかを考える。$|A| \not\equiv 0 \pmod{2n}$ ならば $|A|_{2n} = |A|_n$ だから, $|A| \equiv 0 \pmod{2n}$, 即ち $|A|_{2n} = 2n$ の場合だけを考える。

どちらか一方, 例えば $|C_2|$ が奇数のときは $a_2 = 1$ で, 定理 3.2 より $Z^1(C_2,\langle x\rangle) = \{0\}$ である。よって, $|Z^1(A,\langle x\rangle)| = |Z^1(C_1,\langle x\rangle)| = n$ だから, このとき (4.2) は成り立たない (このことは定理 5.5 の証明, 命題 6.2, 及び定理 6.4 の注 (2) につながっていく)。

$|C_1|$, $|C_2|$ はともに偶数とする。上の場合分け (i) のときは $|Z^1(A,\langle x\rangle)| \equiv 0 \pmod{|C_1|_n\cdot|C_2|_n}$ であるが, $|C_1|$, $|C_2|$ はともに偶数だから $|C_1|_n\cdot|C_2|_n \equiv 0 \pmod{2n}$ であり, (4.2) は成り立つ。従って, 上の場合分け (ii) で最小値 n を取るときだけ (4.2) は成り立たない。命題 3.7 より,

$$T(a_1)_n\cdot(1-a_1)_n = \begin{cases} 2n & (n\geq 4 \text{ かつ } a_1 = -1) \\ n & (\text{その他}) \end{cases}$$

であるから, それは $|C_1|_n = |a_1|$ (特に $n\geq 4$) かつ $a_1 \neq -1$ のときに限る。ここで補題を一つ用意する。

補題 4.2. $|a_1|\cdot|C_2| \equiv 0 \pmod{2n}$, $a_1 \neq 1$ とすると, $\mathbb{Z}_n$ において

$$(T(a_1)) \subset (1+a_1)\,\mathrm{Ann}_{\mathbf{Z}_n}(\frac{|C_2|}{|a_2|}T(a_2))$$

証明. 命題 3.7 より, $\dfrac{T(a_1)_n}{|a_1|} = \dfrac{(1+a_1)_n}{2}$ であったから,

$$(T(a_1)) = (1+a_1)\left(\frac{|a_1|}{2}\right) \subset (1+a_1)\operatorname{Ann}_{\mathbf{Z}_n}(|C_2|) \subset (1+a_1)\operatorname{Ann}_{\mathbf{Z}_n}(\frac{|C_2|}{|a_2|}T(a_2)) \qquad \square$$

定理 4.3. $|C_1|$, $|C_2|$ はともに偶数とする。このとき, $\left|Z^1(A,\langle x\rangle)\right| \not\equiv 0 \pmod{|A|_{2n}}$ であるためには, 次の 2 条件を満たすことが必要十分である:

(1) $|A| \equiv 0 \pmod{2n}$。
(2) $i = 1,2$ のどちらかが $|C_i|_n = |a_i|$ (特に $a_i \neq 1$ で $n \geq 4$), かつ $a_i \neq -1$ を満たす。

更にこのとき $\left|Z^1(A,\langle x\rangle)\right| = n$ である。

証明. 必要性は示したので, 十分性を示す。$|A| \equiv 0 \pmod{2n}$ かつ $|C_1|_n = |a_1|$, $a_1 \neq -1$ とする。命題 3.7 より,

$$(1-a_2)\operatorname{Ann}_{\mathbf{Z}_n}(\frac{|C_1|}{|a_1|}T(a_1)) = (1-a_2)(1-a_1) \subset (1-a_1)\operatorname{Ann}_{\mathbf{Z}_n}(\frac{|C_2|}{|a_2|}T(a_2))$$

だから, このときは仮定 (4.1) の場合となる。更に, 補題 4.2 より,

$$\operatorname{Ann}_{\mathbf{Z}_n}(1-a_1) = (T(a_1)) \subset (1+a_1)\operatorname{Ann}_{\mathbf{Z}_n}(\frac{|C_2|}{|a_2|}T(a_2)) \subsetneq \operatorname{Ann}_{\mathbf{Z}_n}(\frac{|C_2|}{|a_2|}T(a_2)) \tag{4.3}$$

であるから, 先の (ii) の場合になる。よって, $\left|Z^1(A,\langle x\rangle)\right| = T(a_1)_n \cdot (1-a_1)_n = n$ となる。 $\square$

注. 式 (4.3) の最後が真部分集合になるのは $0 \neq T(a_1) \in \operatorname{Ann}_{\mathbf{Z}_n}(\frac{|C_2|}{|a_2|}T(a_2))$ からわかる。特に, このときは場合分け (i) にはならない。

5 $Z^1(C, D_{2n})$

n は 2 巾で 4 以上とする。まず, 位数 $2n$ の二面体群

$$G = D_{2n} = \langle x, y \mid x^n = y^2 = (xy)^2 = 1\rangle$$

の自己同型とその位数をすべて決めたい。$b \in \mathbb{Z}_n$, $a \in U(\mathbb{Z}_n)$ に対し, $\sigma_{b,a} \in \operatorname{Aut}(G)$ を

$$\sigma_{b,a} : x \mapsto x^a, \quad y \mapsto x^b y$$

で定めると,

$$\operatorname{Aut}(G) = \{\sigma_{b,a} \mid b \in \mathbb{Z}_n,\ a \in U(\mathbb{Z}_n)\} \simeq \mathbb{Z}_n \rtimes U(\mathbb{Z}_n), \qquad \sigma_{b,a} \mapsto (b,a)$$

であることが容易にわかる (ここで $U(\mathbb{Z}_n)$ の $\mathbb{Z}_n$ 上の作用は自然なもの)。$(b,a) \in \mathbb{Z}_n \rtimes U(\mathbb{Z}_n)$ の位数とは

$$\langle c\rangle \to \mathbb{Z}_n \rtimes U(\mathbb{Z}_n), \qquad c \mapsto (b,a)$$

が準同型となるような巡回群 $\langle c\rangle$ の位数の最小値であり, 定理 2.1 からそれは c が $\mathbb{Z}_n$ 上 a として作用でき,

$$\langle c\rangle \to \mathbb{Z}_n, \qquad c \mapsto b$$

がコサイクルとなるような位数 $|c|$ の最小値でもある。定理 3.2 から, それは

$$|a| \mid |c|, \qquad \frac{|c|}{|a|}T(a)b = 0 \quad (\text{in } \mathbb{Z}_n)$$

となる $|c|$ の最小値なので, (§3 の応用の一つとして) 次を得る。

補題 5.1. $|\sigma_{b,a}| = \dfrac{|a|\,n}{(T(a)b)_n}$ である。特に, その最大値 $\exp \mathrm{Aut}(G)$ は n である。

さて, 有限巡回群 $C = \langle c \rangle$ が G に $c \mapsto \sigma_{b,a}$ で作用しているとする。$|a| \mid |\sigma_{b,a}| \mid |C|_n$ に注意する。

$$Z^+(C,G) := \{\zeta \in Z^1(C,G) \mid \zeta(c) \in \langle x \rangle\},$$
$$Z^-(C,G) := \{\zeta \in Z^1(C,G) \mid \zeta(c) \in \langle x \rangle y\}$$

とおくと, $Z^1(C,G) = Z^+(C,G) \cup Z^-(C,G)$ と分割できる。定理 3.4 と命題 3.7 より次がわかる。

命題 5.2. 自然な全単射 $Z^+(C,G) \simeq Z^1(C,\langle x \rangle)$ があり,

$$Z^+(C,G) \simeq \mathrm{Ann}_{\mathbf{Z}_n}\left(\frac{|C|}{|a|}T(a)\right) = \mathrm{Ann}_{\mathbf{Z}_n}\left(|C| \cdot \frac{(1+a)_n}{2}\right)$$
$$|Z^+(C,G)| = \left(\frac{|C|}{|a|}T(a)\right)_n = \left(|C| \cdot \frac{(1+a)_n}{2}\right)_n$$

次に, $Z^-(C,G) \simeq \{x^i y \mid R(x^i y, c, |C|) = 1\}$ を求める。

$$R(x^i y, c, |C|) = x^{\mathrm{tr}_{|C|}(-a)i + \sum_{j=0}^{|C|-1}(-1)^j \mathrm{tr}_j(a)b} y^{|C|}$$

であるから, $c \mapsto x^i y$ となるコサイクルが存在するためには, $|C|$ が偶数でかつ $\mathbf{Z}_n$ において

$$\mathrm{tr}_{|C|}(-a)i + \sum_{j=0}^{|C|-1}(-1)^j \mathrm{tr}_j(a)b = 0 \tag{5.1}$$

が成り立つことが必要十分である。ここで次のような式変形ができる。

補題 5.3. 一般に自然数 r と $a \in \mathbf{Z}_n$ に対して, $\displaystyle\sum_{j=0}^{2r-1}(-1)^j \mathrm{tr}_j(a) = -\mathrm{tr}_r(a^2)$

従って $|C|$ が偶数のとき, 条件式 (5.1) は $\mathbf{Z}_n$ における等式 $\mathrm{tr}_{|C|}(-a)i = \mathrm{tr}_{|C|/2}(a^2)b$, 即ち

$$\frac{|C|}{|-a|}T(-a)i = \frac{|C|}{2\,|a^2|}T(a^2)b \tag{5.2}$$

に書き直せる。そこで,

$$S(a) := \mathrm{tr}_{|C|/2}(a^2) = \frac{|C|}{2\,|a^2|}T(a^2)$$

とおく。$a \neq -1$ のとき, $|-a| = 2\,|a^2|$, $T(-a) = (1-a)T(a^2)$ (補題 3.1) であるから, 等式 (5.2) は

$$S(a)(1-a)i = S(a)b \tag{5.3}$$

と変形できる。他方, $a = -1$ のときも $S(-1) = |C|/2$ であるから, やはり (5.3) に変形できる。

さて, $a^2 \in \langle 5 \rangle$ より $T(a^2)_n = |a^2|$ である (命題 3.6) から, $\mathbf{Z}_n$ のイデアルとして

$$(S(a)) = \left(\frac{|C|}{2}\right), \quad \mathrm{Ann}_{\mathbf{Z}_n}(S(a)) = \left(\frac{n}{(|C|/2)_n}\right)$$

である。従って, 式 (5.3) は結局

$$(1-a)i \equiv b \mod \left(\frac{n}{(|C|/2)_n}\right)$$

となる。また, このような $i \in \mathbf{Z}_n$ が存在するためには

$$b \in (1-a)\mathbf{Z}_n + \mathrm{Ann}_{\mathbf{Z}_n}(S(a)) = \left(1-a,\ \frac{n}{(|C|/2)_n}\right)$$

が必要十分である。ここまでまとめて次を得る。

命題 5.4. $Z^-(C,G)\neq\emptyset$ となるためには

$$|C|\equiv 0 \pmod 2 \quad \text{かつ} \quad b\in\left(1-a,\ \frac{n}{(|C|/2)_n}\right)$$

が必要十分であり, このとき,

$$Z^-(C,G)\simeq\{i\in\mathbb{Z}_n \mid \mathrm{tr}_{|C|}(-a)i=\mathrm{tr}_{|C|/2}(a^2)b\}=\left\{i\in\mathbb{Z}_n \;\middle|\; (1-a)i\equiv b \mod\left(\frac{n}{(|C|/2)_n}\right)\right\},$$

$$|Z^-(C,G)|=\left(\frac{|C|}{|-a|}T(-a)\right)_n=\left(|C|\cdot\frac{(1-a)_n}{2}\right)_n$$

以上, 条件式 (5.1) から, $Z^-(C,G)$ は空集合であるか, もしくは $\mathbb{Z}_n$ の $\mathrm{Ann}_{\mathbb{Z}_n}(\mathrm{tr}_{|C|}(-a))$ による一つの剰余類と全単射があることがわかった。また, (5.1) を $\mathbb{Z}_n$ におけるより簡潔な条件式に変形した。その結果, データ $(|C|,n,a,b)$ を実際に与えれば, $Z^1(C,G)$ は集合として具体的に書き下せるようにもなった。しかし, 実は 0 でない $|Z^-(C,G)|$ に関しては, (5.1) を解析せずとも, 次のことからすぐわかってしまうのである。

今, c の作用が $\sigma_{b,a}$ のときの G を $G_{b,a}$ と書くことにする。もし $\zeta(c)=x^iy$ となる $\zeta\in Z^1(C,G_{b,a})$ が存在すれば, 定理 2.5 (作用の取り換え) により

$$\zeta_r\colon Z^1(C,G_{2i-b,-a})\to Z^1(C,G_{b,a}),\qquad \eta\mapsto\eta\cdot\zeta$$

は全単射となる。Z^+ や Z^- の定義から, ζ_r は全単射

$$Z^+(C,G_{2i-b,-a})\simeq Z^-(C,G_{b,a}),$$
$$Z^-(C,G_{2i-b,-a})\simeq Z^+(C,G_{b,a})$$

を引き起こす。従って,

$$|Z^-(C,G_{b,a})|=|Z^+(C,G_{2i-b,-a})|=|\mathrm{Ann}_{\mathbb{Z}_n}(\mathrm{tr}_{|C|}(-a))|=\left(|C|\cdot\frac{(1-a)_n}{2}\right)_n$$

を得る。

このように $|Z^-(C,G)|$ を「作用の取り換え」から求めようとする場合, $Z^-(C,G)$ がいつ空集合となるかを判定することが重要となる。この観点に立つと, 命題 5.4 における計算はその必要十分条件をも与えているところに価値があり, それは現在のところ上のような計算によるしかない。

さて, 本節の設定で予想が正しいことを確かめる。

定理 5.5. $|Z^1(C,G)|=|Z^+(C,G)|+|Z^-(C,G)|\equiv 0 \pmod{|C|_{2n}}$。

証明. c の作用を $\sigma_{b,a}$ とする。$|Z^1(C,G)|$ は $Z^-(C,G)$ が空集合となるか否かに応じて,

$$\left(|C|\cdot\frac{(1+a)_n}{2}\right)_n \quad \text{または} \quad \left(|C|\cdot\frac{(1+a)_n}{2}\right)_n+\left(|C|\cdot\frac{(1-a)_n}{2}\right)_n$$

となり, 何れも $|C|_n$ で割り切れる。$|C|\not\equiv 0 \pmod{2n}$ のときは $|C|_{2n}=|C|_n$ だからよい。$|C|\equiv 0 \pmod{2n}$ のときは, 命題 5.4 より $Z^-(C,G)\neq\emptyset$ であり, $|Z^+(C,G)|=|Z^-(C,G)|=n$ となり, $|Z^1(C,G)|=2n$ を得る。 □

6 $Z^1(C_1\times C_2, D_{2n})$

n は 2 巾で 4 以上とする。$C_1=\langle c_1\rangle$, $C_2=\langle c_2\rangle$ を有限巡回群とし, $A=C_1\times C_2$ が位数 $2n$ の二面体群 $G=D_{2n}$ に

$$\varphi\colon A\to\mathrm{Aut}(G),\qquad \varphi(c_1)=\sigma_{b_1,a_1},\quad \varphi(c_2)=\sigma_{b_2,a_2}$$

で作用しているものとする。このとき, φ が準同型であることから, b_1,b_2 について次がわかる。

補題 6.1. $|C_1|_n = |a_1|$, $a_1 \neq -1$ とすると,

$$\exists s,t \in \mathbf{Z}_n \quad \text{s.t.} \quad b_1 = (1-a_1)s, \quad b_2 = (1-a_2)s + tT(a_1)$$

証明. $|a_1| \,|\, |\sigma_{b_1,a_1}| \,|\, |C_1|_n$ であるが, 仮定より $|a_1| = |\sigma_{b_1,a_1}| = |C_1|_n$ である。補題 5.1 より,

$$|\sigma_{b_1,a_1}| = \frac{|a_1|\,n}{(T(a_1)b_1)_n}$$

であったから, $(T(a_1)b_1)_n = n$ である。$a_1 \neq -1$ より, $b_1 \in \mathrm{Ann}_{\mathbf{Z}_n}(T(a_1)) = (1-a_1)$ であるから,

$$\exists s \in \mathbf{Z}_n \quad \text{s.t.} \quad b_1 = (1-a_1)s$$

更に, σ_{b_1,a_1} と σ_{b_2,a_2} の可換性より,

$$(1-a_1)b_2 = (1-a_2)b_1 = (1-a_2)(1-a_1)s$$

よって $b_2 \equiv (1-a_2)s \mod \mathrm{Ann}_{\mathbf{Z}_n}(1-a_1) = (T(a_1))$ であるから補題がいえる。 □

さて, $Z^1(A,G)$ に関する予想を確かめる。例 2.4 から, コサイクル $\zeta\colon A \to G$ を与えることと,

$$\zeta_1 \in Z^1(C_1,G), \qquad \zeta_2 \in Z^1(C_2,G), \qquad \zeta_1(c_1)\cdot {}^{c_1}\zeta_2(c_2) = \zeta_2(c_2)\cdot {}^{c_2}\zeta_1(c_1) \tag{6.1}$$

となる ζ_1, ζ_2 を与えることとは同値である。

もし $|C_2|$ が奇数ならば, $\sigma_{b_2,a_2} = 1$ であり, 命題 5.2, 命題 5.4 から $Z^1(C_2,G)$ は自明な写像のみからなる。特に, 条件式 (6.1) から $Z^1(A,G) \simeq Z^1(C_1,G)$ である。定理 5.5 と合わせて次を得る。

命題 6.2. $|C_2|$ が奇数のときは, $\left|Z^1(A,G)\right| = \left|Z^1(C_1,G)\right| \equiv 0 \pmod{|A|_{2n}}$。

以下, $|C_1|$, $|C_2|$ はともに偶数とする。A は $\langle x\rangle$ に $c_1 \mapsto a_1$, $c_2 \mapsto a_2$ で作用している。この $\langle x\rangle$ を $\langle x\rangle_{a_1,a_2}$ と書く。前と同様に, $Z^1(A,G)$ の分割

$$\begin{aligned}
Z^{++}(A,G) &:= \left\{\zeta \in Z^1(A,G) \mid \zeta|_{C_1} \in Z^+(C_1,G),\ \zeta|_{C_2} \in Z^+(C_2,G)\right\} \simeq Z^1(A,\langle x\rangle_{a_1,a_2}),\\
Z^{-+}(A,G) &:= \left\{\zeta \in Z^1(A,G) \mid \zeta|_{C_1} \in Z^-(C_1,G),\ \zeta|_{C_2} \in Z^+(C_2,G)\right\},\\
Z^{+-}(A,G) &:= \left\{\zeta \in Z^1(A,G) \mid \zeta|_{C_1} \in Z^+(C_1,G),\ \zeta|_{C_2} \in Z^-(C_2,G)\right\},\\
Z^{--}(A,G) &:= \left\{\zeta \in Z^1(A,G) \mid \zeta|_{C_1} \in Z^-(C_1,G),\ \zeta|_{C_2} \in Z^-(C_2,G)\right\}
\end{aligned}$$

を考える。もし, 例えば $Z^{-+}(A,G) \neq \emptyset$ ならば, $\zeta \in Z^{-+}(A,G)$ を一つ固定し, $\zeta(c_1) = x^{i_1}y$, $\zeta(c_2) = x^{i_2}$ とおけば, 定理 2.5 (作用の取り換え) から,

$$\zeta * \varphi\colon A \to \mathrm{Aut}(G), \qquad c_1 \mapsto \sigma_{2i_1-b_1,-a_1}, \quad c_2 \mapsto \sigma_{2i_2+b_2,a_2}$$

は新しい作用となり, $\zeta_r\colon Z^1(A,G_{\zeta*\varphi}) \to Z^1(A,G)$ は四つの全単射

$$\begin{cases}
Z^{++}(A,G_{\zeta*\varphi}) & \to & Z^{-+}(A,G),\\
Z^{-+}(A,G_{\zeta*\varphi}) & \to & Z^{++}(A,G),\\
Z^{+-}(A,G_{\zeta*\varphi}) & \to & Z^{--}(A,G),\\
Z^{--}(A,G_{\zeta*\varphi}) & \to & Z^{+-}(A,G)
\end{cases}$$

を引き起こす。よって,

$$\left|Z^{-+}(A,G)\right| = \left|Z^{++}(A,G_{\zeta*\varphi})\right| = \left|Z^1(A,\langle x\rangle_{-a_1,a_2})\right| \tag{6.2}$$

となる。定理 4.3 から, この値は $|A|_{2n}$ で割れているか, または n である。このことは $Z^{+-}(A,G)$ や $Z^{--}(A,G)$ についても同様である。従って, $Z^1(A,G)$ について予想を確かめるには, これら四つの $|Z^{**}(A,G)|$ のうち $|A|_{2n}$ で割れない (特に 0 ではない) ものが幾つあるかが焦点となる。

命題 6.3. $|C_1|$, $|C_2|$ はともに偶数で, $|Z^{++}(A,G)| \not\equiv 0 \pmod{|A|_{2n}}$ とすると, $Z^{-+}(A,G) \neq \emptyset$ である。

証明. 定理 4.3 より, $|A| \equiv 0 \pmod{2n}$ かつ $k = 1, 2$ のどちらかは $|C_k|_n = |a_k|$, $a_k \neq \pm 1$ を満たす。また, コサイクル $A \to G$ で, $c_1 \mapsto x^{i_1}y$, $c_2 \mapsto x^{i_2}$ となるものが存在するための必要十分条件は, 条件 (6.1) を命題 5.2, 命題 5.4 を用いて書き換えると, 次のようになる。

$$\text{(I)} \quad (1-a_1)i_1 \equiv b_1 \mod \mathrm{Ann}_{\mathbf{Z}_n}(\frac{|C_1|}{2}),$$

$$\text{(II)} \quad i_2 \in \mathrm{Ann}_{\mathbf{Z}_n}(\frac{|C_2|}{|a_2|}T(a_2)),$$

$$\text{(III)} \quad (1-a_2)i_1 - b_2 = (1+a_1)i_2$$

(1) $|C_1|_n = |a_1|$, $a_1 \neq \pm 1$ の場合。

補題 6.1 より,

$$\exists s, t \in \mathbb{Z}_n \quad \text{s.t.} \quad b_1 = (1-a_1)s, \quad b_2 = (1-a_2)s + tT(a_1)$$

である。従って, 条件 (I) の i_1 として s をとることができ, このとき条件 (II), (III) は

$$i_2 \in \mathrm{Ann}_{\mathbf{Z}_n}(\frac{|C_2|}{|a_2|}T(a_2)) \quad \text{かつ} \quad -tT(a_1) = (1+a_1)i_2$$

となる。補題 4.2 より $(T(a_1)) \subset (1+a_1)\,\mathrm{Ann}_{\mathbf{Z}_n}(\frac{|C_2|}{|a_2|}T(a_2))$ であるから, 確かにこのような i_2 が存在し, $Z^{-+}(A,G) \neq \emptyset$ がわかる。

(2) $|C_2|_n = |a_2|$, $a_2 \neq \pm 1$ の場合。

補題 6.1 より,

$$\exists s, t \in \mathbb{Z}_n \quad \text{s.t.} \quad b_2 = (1-a_2)s, \quad b_1 = (1-a_1)s + tT(a_2)$$

である。命題 3.7 より

$$T(a_2)_n \cdot \frac{|C_1|}{2} = \frac{(1+a_2)_n}{2} \cdot \frac{|a_2| \cdot |C_1|}{2} \equiv 0 \pmod{n}$$

だから, $T(a_2) \in \mathrm{Ann}_{\mathbf{Z}_n}(\frac{|C_1|}{2})$ となる。従って, 条件 (I) の i_1 として s がとれる。このとき, i_2 として 0 をとると条件 (II), (III) を満たすから, $Z^{-+}(A,G) \neq \emptyset$ がわかる。 □

定理 6.4. $|C_1|$, $|C_2|$ がともに偶数ならば, 次の何れかが成り立つ。

$$\begin{cases} |Z^{++}(A,G)| \equiv |Z^{-+}(A,G)| \equiv |Z^{+-}(A,G)| \equiv |Z^{--}(A,G)| \equiv 0 \pmod{|A|_{2n}} \\ |Z^{++}(A,G)| = |Z^{-+}(A,G)| = |Z^{+-}(A,G)| = |Z^{--}(A,G)| = n \end{cases}$$

証明. $|Z^{**}(A,G)|$ のうち $|A|_{2n}$ で割れない (特に空集合でない) ものが一つでもあれば, 作用を取り換えて, それは $|Z^{++}(A,G)|$ としてよい。このとき, 組 (C_1, C_2, a_1, a_2) は定理 4.3 の条件を満たし, $|Z^{++}(A,G)| = n$ である。

命題 6.3 より $Z^{-+}(A,G) \neq \emptyset$ だから, $\zeta \in Z^{-+}(A,G)$ を一つとれる。このとき, 前述の等式 (6.2) より $|Z^{-+}(A,G)| = |Z^{++}(A,G_{\zeta*\varphi})| = |Z^1(A, \langle x \rangle_{-a_1,a_2})|$ である。組 $(C_1, C_2, -a_1, a_2)$ はやはり定理 4.3 の条件を満たすので, $|Z^{-+}(A,G)| = n$ が一般にいえる。$A = C_2 \times C_1$ と見てこのことを適用すると, $|Z^{+-}(A,G)| = n$ も一般にいえる。更に, 以上のことを $|Z^{++}(A,G_{\zeta*\varphi})| = n$ に適用すると, $|Z^{--}(A,G)| = |Z^{+-}(A,G_{\zeta*\varphi})| = n$ を得る。 □

注. (1) 上の定理の二式が同時に成り立つこともある。第一式が成り立つかどうかは定理 4.3 で判定できる。(2) 何れか一方, 例えば $|C_2|$ が奇数のときは $Z^1(A,G) \simeq Z^1(C_1,G)$ であるから, $Z^{+-}(A,G) = Z^{--}(A,G) = \emptyset$ であり,

$$\begin{cases} |Z^{++}(A,G)| \equiv |Z^{-+}(A,G)| \equiv 0 \pmod{|A|_{2n}} & (|A| \not\equiv 0 \pmod{2n} \text{ のとき}) \\ |Z^{++}(A,G)| = |Z^{-+}(A,G)| = n & (|A| \equiv 0 \pmod{2n} \text{ のとき}) \end{cases}$$

以上のことから, 本節の設定でも予想が成り立つことがわかった。

定理 6.5. $|Z^1(A,G)| \equiv 0 \pmod{|A|_{2n}}$。

参考文献

[1] T. Asai and Y. Takegahara, *On the number of crossed homomorphisms*, Hokkaido Math. J. **28** (1999), 535–543.

[2] ———, |Hom(A,G)|, IV, J. Algebra (to appear).

[3] T. Asai and T. Yoshida, |Hom(A,G)|, II, J. Algebra **160** (1993), 273–285.

[4] R. Brauer, *On a theorem of Frobenius*, Amer. Math. Monthly **76** (1969), 562–565.

[5] K. Brown, *Cohomology of Groups*, Graduate Texts in Math., vol. 87, Springer-Verlag, 1982.

[6] W. Burnside, *The Theory of Groups of Finite Order*, 2nd ed., Cambridge University Press, 1907.

[7] C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, 2nd ed., Pure and Appl. Math., Interscience Publishers, New York, 1966.

[8] M. Hall, *The Theory of Groups*, MacMillan, New York, 1959.

[9] P. Hall, *On a theorem of Frobenius*, Proc. London Math. Soc. (2) **40** (1935), 468–501.

[10] T. Yoshida, |Hom(A,G)|, J. Algebra **156** (1993), 125–156.

[11] H. Zassenhaus, *The Theory of Groups*, 2nd ed., Chelsea Publishing Company, New York, 1958.

[12] 鈴木 通夫, 群論 (上), 岩波書店, 1977.

[13] 竹ヶ原 裕元, *On P. Hall's relations in finite groups*, 群論とその周辺—総括と展望, 京都大学数理解析研究所講究録, no. 1214, 2001, pp. 27–36.